

WHAT IS CLAIMED IS:

1. An apparatus for securing communication information in CDMA communication system comprising:

a vocoder encoding the input analog signal as an information bit having a predetermined size and generating a vocoder packet information bit;

an encryptor encrypting the vocoder packet information bit from said vocoder;

a CDMA framer adding a frame quality indicator and the encoder tail bits to the encrypted vocoder packet information bit from said encryptor to configure as a CDMA frame;

a CDMA frame transmitter transmitting the CDMA frame which passes a convolutional encoder, interleaver, and modulator in sequence, to a base station through an assigned frequency band;

a CDMA frame receiver receiving a signal from the base station and reproducing the CDMA frame;

a CDMA deframer extracting the encrypted vocoder packet information bit from the CDMA frame reproduced by said CDMA frame receiver;

a decryptor decrypting the encrypted vocoder packet information bit extracted by said CDMA deframer; and

a vocoder decoding the decrypted vocoder packet information bit from said decryptor as an analog signal,

wherein said encryptor encrypts the vocoder packet information bit using a block cipher and a security key, said decryptor decrypts the encrypted vocoder packet information bit using said block cipher and a security

key shared with the other mobile.

2. The apparatus according to claim 1, wherein the block cipher is DES.

3. The apparatus according to claim 1, wherein said encryptor performs or bypasses the encryption by a security mode that a user enters.

4. The apparatus according to claim 3, wherein said encryptor generates a predetermined pattern corresponding to the security mode ON or OFF and adds the generated pattern to the information bit of the traffic channel and transmits it to the other mobile, wherein said decryptor performs or bypasses the decryption by said pattern.

5. The apparatus according to claim 4, wherein said encryptor adds the security key to the information bit of the traffic channel when the security mode is set to ON, wherein said decryptor decrypts the encrypted vocoder packet information bit by said security key included in the information bit of the traffic channel.

6. The apparatus according to claim 4, wherein said encryptor encrypts the security key by a master key when the security mode is set to ON and adds the encrypted security key to the information bit of the traffic channel, wherein said decryptor decrypts the encrypted security key included in the information bit of the traffic channel by said master key, and decrypts the encrypted vocoder packet information bit by the decrypted security key.

7. The apparatus according to claim 4, wherein said encryptor is provided with multiple security keys and adds an index of the security key selected among the multiple

security keys to the information bit of the traffic channel when the security mode is set to ON, and encrypts the vocoder packet information bit by the selected security key, wherein said decryptor shares the multiple security keys provided in said encryptor, and decrypts the encrypted vocoder packet information bit using the security key selected by the index included in the information bit of the traffic channel.

8. The apparatus according to claim 1, wherein said vocoder in a reverse traffic channel generates a signal MUTE\_Tx indicating the mute status of the generated vocoder packet information bit, wherein said encryptor does not encrypt the vocoder packet information bit if the MUTE\_Tx indicates the mute, wherein said CDMA deframer generates a signal MUTE\_Rx indicating the mute status of the encrypted vocoder packet information bit, wherein said decryptor does not decrypts the encrypted vocoder packet information bit if the MUTE\_Rx indicates the mute.

9. The apparatus according to claim 1, wherein said encryptor encrypts all or the part of the vocoder packet information bits, wherein said decryptor decrypts all or the part of the encrypted vocoder packet information bits.

10. A method for securing communication information in CDMA communication system comprising the steps of:

encoding a input analog signal as an information bit having a predetermined size and generating a vocoder packet information bit;

encrypting said encoded vocoder packet information bit using a block cipher and a security key;

adding a frame quality indicator and the encoder tail bits to the encrypted vocoder packet information bit and configuring it as a CDMA frame; and

transmitting the CDMA frame which passes a convolutional encoder, interleaver, and modulator in sequence, to a base station through an assigned frequency band.

11. The method according to claim 10, wherein said block cipher is DES.

12. The method according to claim 10, wherein said step of encrypting comprises the step of performing or bypassing the encryption by a security mode that a user enters.

13. The method according to claim 12, wherein said step of encrypting comprises the steps of generating a predetermined pattern corresponding to the security mode ON or OFF and adding the pattern to the information bit of the traffic channel.

14. The method according to claim 13, wherein said step of encrypting comprises the step of adding said security key to the information bit of the traffic channel when the security mode is set to ON.

15. The method according to claim 13, wherein said step of encrypting comprises the step of encrypting the security key by a predetermined master key when the security mode is set to ON and adding the encrypted security key to the information bit of the traffic channel.

16. The method according to claim 13, wherein said step of encrypting comprises the step of adding an index of the security key selected among multiple security keys

to the information bit of the traffic channel when the security mode is set to ON, and encrypting said vocoder packet information bit using the selected security key.

17. The method according to claim 10, wherein said step of encrypting comprises the steps of detecting the mute status of the generated vocoder packet information bit, and unencrypting the vocoder packet information bit if the mute is detected.

18. The method according to claim 10, wherein said step of encrypting comprises the step of encrypting only the part of the vocoder packet information bits.

19. A method for securing communication information in CDMA communication system comprising the steps of:

receiving a signal from a base station, and reproducing it as a CDMA frame;

extracting an encrypted vocoder packet information bit from the reproduced CDMA frame;

decrypting the encrypted vocoder packet information bit by a block cipher and a security key; and

decoding the decrypted vocoder packet information bit.

20. The method according to claim 19, wherein said block cipher is DES.

21. The method according to claim 19, wherein said step of decrypting comprises the steps of setting a security mode to ON or OFF according to the predetermined pattern included in the received information bit of the traffic channel, and determining according to the security mode whether the decryption process is to be performed or not.

22. The method according to claim 21, wherein said

security key is that included in the information bit of the traffic channel received when the security mode is set to ON.

23. The method according to claim 21, wherein said security key is that included in the information bit of the traffic channel received when the security mode is set to ON and decrypted by the predetermined master key

24. The method according to claim 21, wherein said security key is that determined by an index included in the information bit of the traffic channel when the security mode is set to ON, among multiple security keys provided in the mobile.

25. The method according to claim 19, wherein said step of decrypting comprises the steps of detecting the mute status of the encrypted vocoder packet information bit, and undecrypting the encrypted vocoder packet information bit if the mute is detected.

26. The method according to claim 19, wherein said step of decrypting comprises the step of decrypting only the part of the the encrypted vocoder packet information bit.